CalWatchdog.com

CalPERS reacts to Anthem security breach

By John Seiler

February 5, 2015

The hacker attack on health insurance provider Anthem Blue Cross announced last night in particular affects hundreds of thousands of members of the California Public Employees' Retirement System. But a security expert told CalWatchdog.com the breach is not critical — provided those affected take precautions.

The attack on Anthem comes on the heels of similar breaches of data for Target, Home Depot and other companies.

Anthem President and CEO Joseph Swedish wrote in a letter to members:

"Anthem was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information, such as claims, test results or diagnostic codes were targeted or compromised.

"Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

"Anthem's own associates' personal information – including my own – was accessed during this security breach."

CalPERS concern

In an email obtained by CalWatchdog.com, Rita L. Gallardo, division chief of CalPERS' Office of Stakeholder Relations, wrote earlier today to those affected:

"As many of you have heard in the news, our health plan partner Anthem Blue Cross disclosed late last night that hackers breached its computer systems and the personal information of its members. Like you, we are very concerned and frustrated about this unacceptable breach. We

have been in touch with Anthem this morning to ensure they are doing everything possible to protect our members and their families who are enrolled in the plan."

Precautions

The hacker attack should not seriously affect Anthem members, whether or not they are part of CalPERS — provided people take precautions, Jim Harper told CalWatchdog.com; he's a senior fellow in information studies at the Cato Institute.

He said that even if hackers obtain Social Security numbers, "it actually isn't that serious because identity fraud takes a lot of work to pull off. When 80 million sets of ID are stolen, that doesn't mean there will be 80 million incidents of identity fraud."

The real risk now, he warned, is to make sure hackers don't use the Anthem news itself as a way to trick people. As the Anthem and CalPERS statements quoted above indicate, members will be notified about the attack, and about what they can do.

Harper said people might get so tired of responding to legitimate inquires that, when a hacker inquiry pops up, they complacently could think, "Oh, not another one! All right, I'll fill out the form and give them the information" — which then is use by the hacker for a serious security breach.

He urged Anthem members to change their passwords often to prevent identity theft. Which is good advice as well for those not part of Anthem, and for any system involving passwords.

CalPERS activism

CalPERS, the country's largest retirement system, also is known for its shareholder activism, such as discouraging what it considers "excessive CEO pay" by companies. CalPERS maintains its activism helps improve company performance and is for the overall betterment of society.

Critics say such activism can reduce investment values, with the taxpayers who ultimately backstop CalPERS' investments put on the hook for any shortfalls.

It's too early to know, but Harper said the Anthem security breach might spark CalPERS' activism in this area, in particular ensuring that "consumers have a right to know a breach has occurred. That sounds good. Yet it's not necessarily good for consumers."

He said that, given the ongoing security breaches, with more expected in the future, "If you hear about it all the time, it creates fear and unease, but not much more security."

Instead, he reiterated that the best policy for consumers is constant vigilance over their own passwords and other data.